# UNITED STATES PATENT AND TRADEMARK OFFICE

3e

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/849,697 | 05/04/2001 | Charles Steven Lingafelt | RSW920010082US1 | 8185 |

| | |
|---|---|
| 7590      04/29/2005 | EXAMINER |
| Jack Friedman | GURSHMAN, GRIGORY |

Jack Friedman
Schmeiser, Olsen, and Watts
3 Lear Jet Lane
Suite201
Latham, NY 12110

| ART UNIT | PAPER NUMBER |
|---|---|
| 2132 | |

DATE MAILED: 04/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

| | Application No. | Applicant(s) |
|---|---|---|
| | 09/849,697 | LINGAFELT ET AL. |
| Office Action Summary | Examiner | Art Unit | |
| | Grigory Gurshman | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *27 December 2004*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-21* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

## DETAILED ACTION

### *Response to Arguments*

1.     Applicant's amendment of claims 1 and 3-8 and the introduction of new claims 13-

21 has necessitated new grounds of rejection.

2.     Applicants arguments have been thoroughly considered but found ~~mute~~ moot in view of

the new grounds of rejection.

### *Claim Rejections - 35 USC § 103*

3.        The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as
> set forth in section 102 of this title, if the differences between the subject matter sought to be
> patented and the prior art are such that the subject matter as a whole would have been obvious
> at the time the invention was made to a person having ordinary skill in the art to which said
> subject matter pertains.  Patentability shall not be negatived by the manner in which the invention
> was made.

4.     Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sherer

(U.S. Patent No. 6.115.376) in view of Glawitsch (U.S. Patent No. 6.772.334 B1) and

further in view of Frantz (U.S. Patent No. 6.697.943 B1).

5.     Referring to claim 1, Sherer discloses a medium access control address

authentication (see abstract and Fig. 4).  Sherer teaches a plurality of ports adapted for

connection to respective MAC layer devices includes storing authentication data in the

star configured interconnection device that maps MAC addresses of end stations in the

network to particular ports on the star configured interconnection device. Upon receiving

a packet on a particular port, the process involves determining whether the packet

carries a source address, which the authentication data maps to the particular port. If

the packet carries a source address, which the authentication data maps to the

particular port, then the packet is accepted. If the packet does not carry a source MAC

address, which the authentication maps to the port, then an authentication protocol is

executed on the port to determine whether the MAC address originates from an

authorized sender according to the authentication protocol (see abstract). According to

Sherer, network devices learn the segments of the network on which to find certain

MAC addresses. Thus, by using the MAC address of another device, an end station is

capable of fooling the network so that packets destined to the end station that it is

mimicking, are routed to the mimic. An unscrupulous user spoofing another packet can

introduce unwanted data such as computer viruses into a packet stream being

transmitted from the end station, or hijack a user's network session and gain

unauthorized access to other system resources  (see column 1, lines 50-65).

6.    Referring to the independent claims 1 the limitation "receiving a

message by the network-addressable device" is met by a packet (102 In

 Fig 4.), which is transmitted to interconnection device (100). The limitation

"detecting a communication protocol violation ..., wherein the

communication protocol violation is indicative of " an attack " by a spoofing vandal using

an identity of the network-addressable device..." is met by teaching that upon receiving

a packet on a particular port, the process involves determining whether the packet

carries a source address, which the authentication data maps to the particular port (see

abstract).  Sherer, however does not explicitly teach that activity by the spoofer is a

denial of service attack.  Referring to claim 1, Glawitsch discloses a system for

preventing spoofed denial of service attack in networked computing environment (see

abstract). Glawitsch teaches generating a request acknowledgement packet with checksum as pseudo sequence number and source address in request packet as destination address. Comparison of the check sums serves as indication of the denial of service attack (see abstract and Fig. 8). Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to use a system for address authentication of Sherer having functionality for determining weather the protocol violation is a denial of service attack by the spoofer using address of a network device as taught in Glawitsch. One of ordinary skill in the art would have been motivated to use a system for address authentication having functionality for determining weather the protocol violation is a denial of service attack by the spoofer using address of a network device as taught in Glawitsch for preventing spoofed denial of service attack (see Glawitsch, abstract).

Sherer and Glawitsch, however do not explicitly teach generating a spoofing alert upon detection of protocol violation. Referring to claim 1, Franz teaches generating spoof control packet, setting the alerts and discarding the packets (see abstract and Fig. 3, blocks 340 and 399). Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to use a system for address authentication having functionality for determining weather the protocol violation is a denial of service attack by the spoofer using address of a network device and generating a spoofing alert as taught in Frantz. One of ordinary skill in the art would have been motivated to use a system for address authentication having functionality for determining weather the protocol violation is a denial of service attack by the spoofer using address of a network device and generating a spoofing alert as taught in Frantz for discarding the packet (see Frantz, Fig.5).

8.      Claims 2-13, 15-21 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Sherer (U.S. Patent No. 6.115.376) in view of Stern (U.S. Patent No. 5.935.249)

and further in view of Frantz (U.S. Patent No. 6.697.943 B1).

9.      Referring to the instant claims, Sherer discloses a medium access control

address authentication (see abstract and Fig. 4). Sherer teaches a plurality of ports

adapted for connection to respective MAC layer devices includes storing authentication

data in the star configured interconnection device that maps MAC addresses of end

stations in the network to particular ports on the star configured interconnection device.

Upon receiving a packet on a particular port, the process involves determining whether

the packet carries a source address, which the authentication data maps to the

particular port. If the packet carries a source address, which the authentication data

maps to the particular port, then the packet is accepted. If the packet does not carry a

source MAC address, which the authentication maps to the port, then an authentication

protocol is executed on the port to determine whether the MAC address originates from

an authorized sender according to the authentication protocol (see abstract).

According to Sherer, network devices learn the segments of the network on which to

find certain MAC addresses. Thus, by using the MAC address of another device, an end

station is capable of fooling the network so that packets destined to the end station that

it is mimicking, are routed to the mimic. An unscrupulous user spoofing another packet

can introduce unwanted data such as computer viruses into a packet stream being

transmitted from the end station, or hijack a user's network session and gain

unauthorized access to other system resources  (see column 1, lines 50-65).

10.   Referring to the independent claim 2, the limitation "receiving a message by the network-addressable device" is met by a packet (102 in Fig 4.), which is transmitted to interconnection device (100). The limitation " detecting a communication protocol violation ..., wherein the communication protocol violation is indicative of activity of a spoofing vandal using an identity of the network-addressable device..." is met by teaching that upon receiving a packet on a particular port, the process involves determining whether the packet carries a source address, which the authentication data maps to the particular port (see abstract).

The limitation "recording attributes of the message" is met by storing the attributes in PORT/MAC table (see Fig.4). Sherer, however, does not explicitly teach advancing the value of a counter associated with the target and comparing the value of the counter with a predetermined threshold.

11.   Referring to the instant claims Stern discloses secure network management function (see abstract). Stern teaches a counter for storing a counter value and the authentication routine for verifying the identity of a user (see column 15, lines 23-25). Stern also teaches checking a value associated with the counter and issuing authorization command if the counter value exceeds a threshold value (see column 16, lines 35-40). Stern, however, does not explicitly teach the command being a spoofing alert. Referring to the instant claims, Franz teaches generating spoof control packet, setting the alerts and discarding the packets (see abstract and Fig. 3, blocks 340 and 399). Therefore at the time the invention was made, it would have been obvious to one of ordinary skill in the art, to modify a system for access control address authentication

of Sherer by using the counter and comparing the value of the counter with

the threshold as taught in Stern and generating a spoofing alert as taught in

Frantz. One ofordinary skill in the art would have been motivated to modify

a system for access control address authentication by using the counter

and comparing the value of the counter with the threshold as taught in

Stern for issuing the authorization command (see Stern

column 16, lines 39-40) and generating a spoofing alert as taught in Frantz

for discarding the packet (see Frantz, Fig.5).

12.    Referring to claims 3-5, 9, 15 and 16, it is well known in the art of

network administration to send  the alert to a network administrator, for

example Windows NT over TCP/IP system use administration alerts.  One

of ordinary skill in the art would have been motivated to send the spoofing

alert to the network administrator for taking an appropriate action such as

blocking the IP address of a sender.

13.    Referring to claim 6, the limitation "blocking the message" is met by

discarding the packet (see Frantz, Fig.5).

14.    Referring to claims 7 and 8, the "spoofing logbook database" is met

by PORT/MAC tables (see Sherer, Fig. 4 unit 100).

15.    Referring to claim 13, it is well known in the art to use Internet as a

communication network, which needs to be protected from spoofing attack.

16.    Referring to claim 20, Sherer teaches that a spoofing vandal may be

connected to the device over the communication network.

17.    Referring to claim 21, generating and comparing function performed by the

network device are met by teaching of Stern: checking a value

associated with the counter and issuing authorization command if the

counter value exceeds a threshold value (see column 16, lines 35-40).

18.     Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sherer

(U.S. Patent No. 6.115.376) in view of Stern (U.S. Patent No. 5.935.249) and further in

in view of Frantz (U.S. Patent No. 6.697.943 B1) and further in view Glawitsch (U.S.

Patent No. 6.772.334 B1)

19.     Referring to claim 14, Sherer, Stern and Frantz teach a system for access control

address authentication using the counter and comparing the value of the counter with

the threshold and generating a spoofing alert. However Sherer, Stern and Frantz do not

teach determining weather the protocol violation is a is a denial of service attack by the

spoofer. Referring to claim 14, Glawitsch discloses a system for preventing spoofed

denial of service attack in networked computing environment (seeabstract).  Glawitsch

teaches generating a request acknowledgement packet with checksum as pseudo

sequence number and source address in request packet as destination address.

Comparison of the check sums serves as indication of the denial of

service attack (see abstract and Fig. 8).   One of ordinary skill in the art would have

been motivated to use a system for address authentication using the counter and

comparing the value of the counter with the threshold and generating a spoofing alert

with functionality for determining weather the protocol violation is a denial of service

attack by the spoofer using address of a network device as taught in Glawitsch for

preventing spoofed denial of service attack (see Glawitsch, abstract).


## Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action.  Accordingly, **THIS ACTION IS MADE FINAL**.  See MPEP

§ 706.07(a).  Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action.  In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action.  In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.


Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Grigory Gurshman whose telephone number is

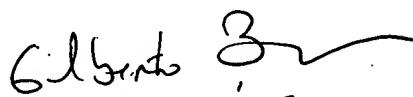(571)272-3803.  The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on (571)272-3799.  The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the
Patent Application Information Retrieval (PAIR) system. Status information for
published applications may be obtained from either Private PAIR or Public PAIR.
Status information for unpublished applications is available through Private PAIR only.
For more information about the PAIR system, see http://pair-direct.uspto.gov. Should
you have questions on access to the Private PAIR system, contact the Electronic
Business Center (EBC) at 866-217-9197 (toll-free).

Grigory Gurshman
Examiner
Art Unit 2132

GG

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100